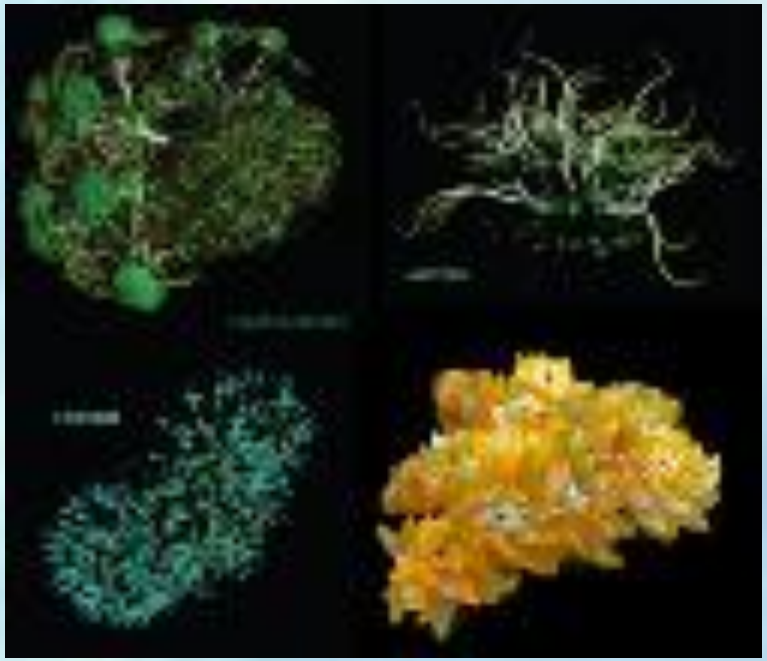
Компьютерные вирусы и антивирусные программы

Что же такое вирус?

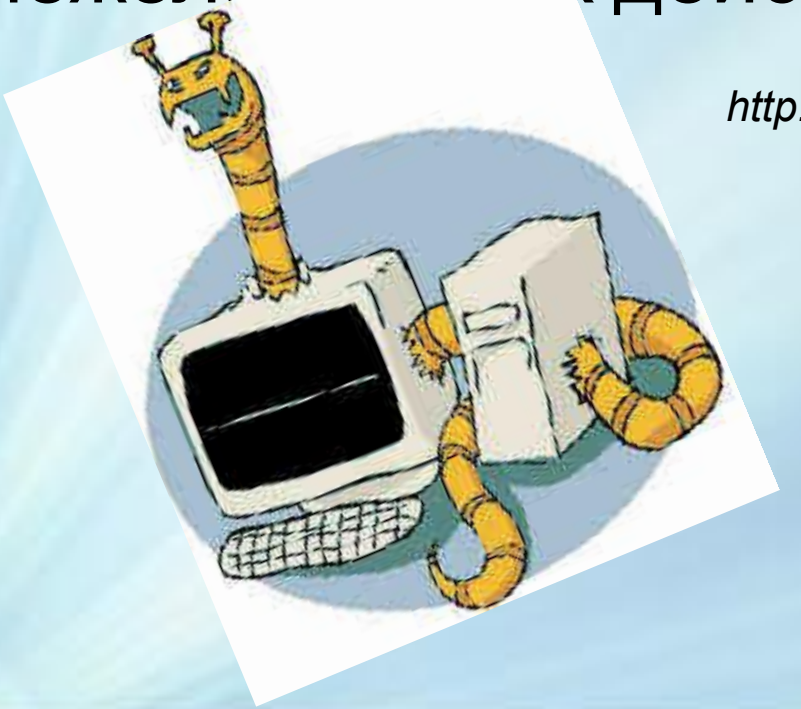
Вирус – мельчайшая неклеточная частица, размножающаяся в живых клетках, возбудитель инфекционного заболевания.



Толковый словарь русского языка
С. И. Ожегова и Н. Ю. Шведовой

Компьютерный вирус – специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелат[illegible]х действий.

Энциклопедия вирусов «Лаборатории Касперского
http://www.viruslist.com/ru/viruses/encyclopedia

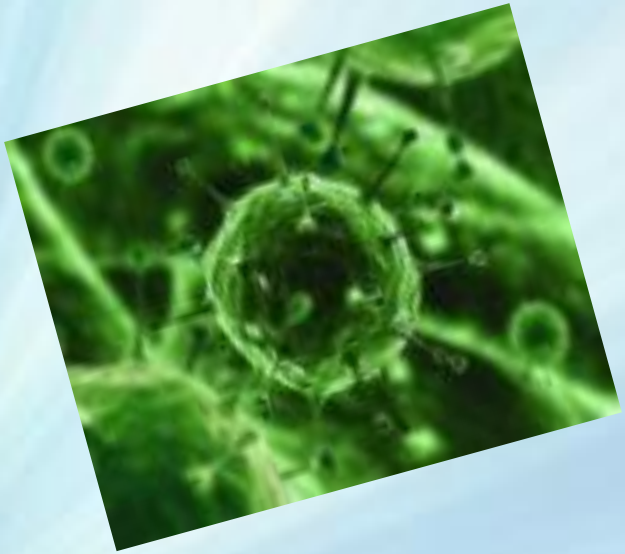


Что же общего между биологическим и компьютерным вирусами?

1. Способность к размножению.
2. Вред для здоровья человека и нежелательные действия для компьютера.
3. Скрытность, т.к. вирусы имеют инкубационный период.

ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Первые исследования саморазмножающихся искусственных конструкций проводилась в середине прошлого столетия учеными Джоном фон Нейманом и Винером.

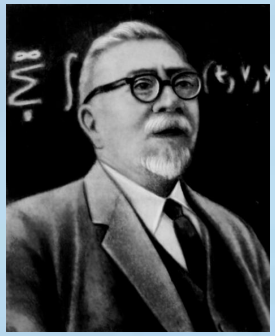


Джон фон Нейман

(1903 - 1957)

Норберт Винер

(1894 - 1964)



ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Первый прототип вируса появился еще в 1971г. Программист Боб Томас, пытаясь решить задачу передачи информации с одного компьютера на другой, создал программу Creeper, самопроизвольно «перепрыгивавшую» с одной машины на другую в сети компьютерного центра.

Правда эта программа не саморазмножалась, не наносила ущерба.

ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

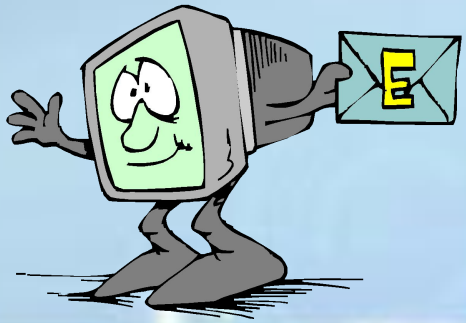
Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») «заражал» дискеты персональных компьютеров. В настоящее время известно несколько десятков тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

ЧЕМ ОПАСЕН КОМПЬЮТЕРНЫЙ ВИРУС?

После заражения компьютера вирус может активизироваться и начать выполнять вредные действия по уничтожению программ и данных.

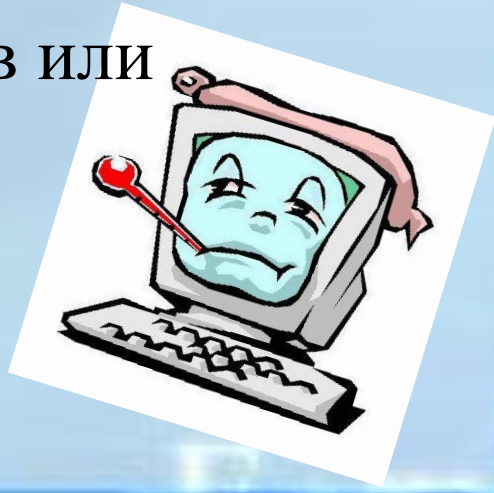
Активизация вируса может быть связана с различными **событиями**:

- *наступлением определённой даты или дня недели*
- *запуском программы*
- *открытием документа…*



Основные признаки проявления вирусов

- Прекращение работы или неправильная работа ранее успешно функционировавших программ
- Медленная работа компьютера
- Невозможность загрузки операционной системы
- Исчезновение файлов и каталогов или искажение их содержимого



Основные признаки проявления вирусов

- Изменение даты и времени модификации файлов
- Изменение размеров файлов
- Частые зависания и сбои в работе компьютера

Основные признаки проявления вирусов

- Неожиданное значительное увеличение количества файлов на диске
- Существенное уменьшение размера свободной оперативной памяти
- Вывод на экран непредусмотренных сообщений или изображений
- Подача непредусмотренных звуковых сигналов

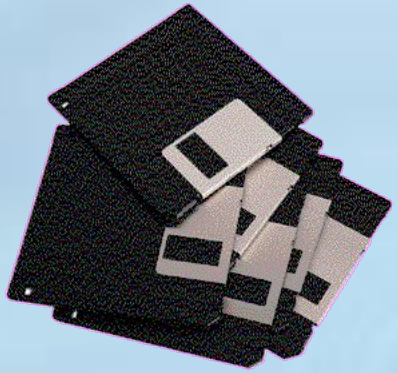
Некоторые характерные признаки поражения вирусом через почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Каналы распространения

Дискеты

Самый распространённый канал заражения в 1980-90 годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов.



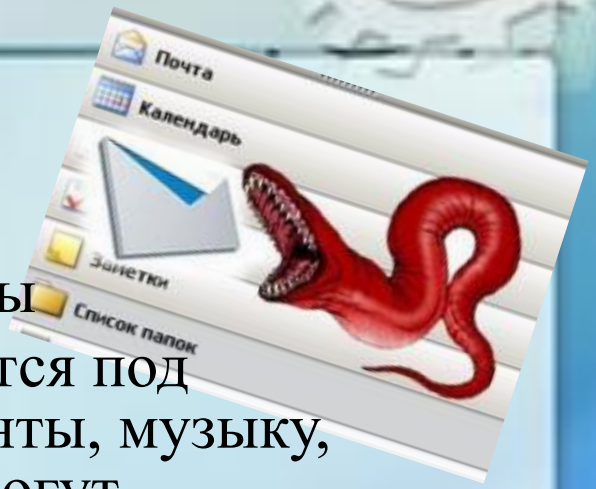
Каналы распространения

Флеш-накопители (флешки)

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла ***autorun.inf,*** в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя.

Флешки — основной источник заражения для компьютеров, не подключённых к сети Интернет.

Каналы распространения



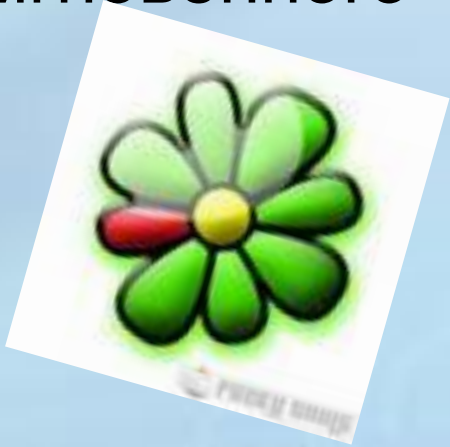
Электронная почта

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

Каналы распространения

Системы обмена мгновенными сообщениями

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

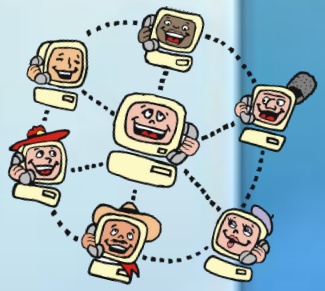


Каналы распространения

Веб-страницы

Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного»

содержимого: скриптов, ActiveX-компоненты, Java-апплетов



Интернет и локальные сети (черви)

Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере

На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.

Каналы распространения

Персональные компьютеры «общего пользования»

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из учащихся принес на своих носителях вирус и заразил какой-либо учебный компьютер, то очередную «заразу» получат и носители всех остальных учащихся, работающих на этом компьютере.

То же относится и к домашним компьютерам, если на них работает более одного человека.

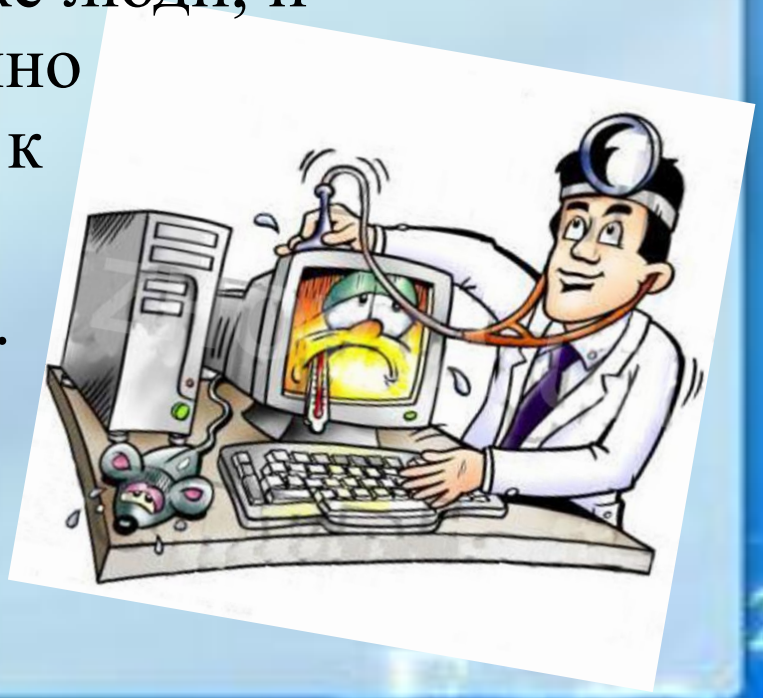
Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска». Часто пиратские копии на дисках содержат файлы, зараженные самыми разнообразными типами вирусов.

Каналы распространения

Ремонтные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники — тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.



По среде обитания:

Файловые вирусы либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы). Находятся в оперативной памяти компьютера и могут заражать другие файлы до момента выключения компьютера или перезагрузки ОС.

Макровирусы заражают файлы документов. Угроза заражения прекращается после закрытия программы.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Методы защиты

- Защита локальных сетей
- Использование дистрибутивного ПО
- Резервное копирование информации
- Использование антивирусных программ
- Не запускать непроверенные файлы

Критерии выбора антивирусных программ

- Надежность и удобство в работе
- Качество обнаружения вирусов
- Существование версий по все популярные платформы
- Скорость работы
- Наличие дополнительных функций и возможностей

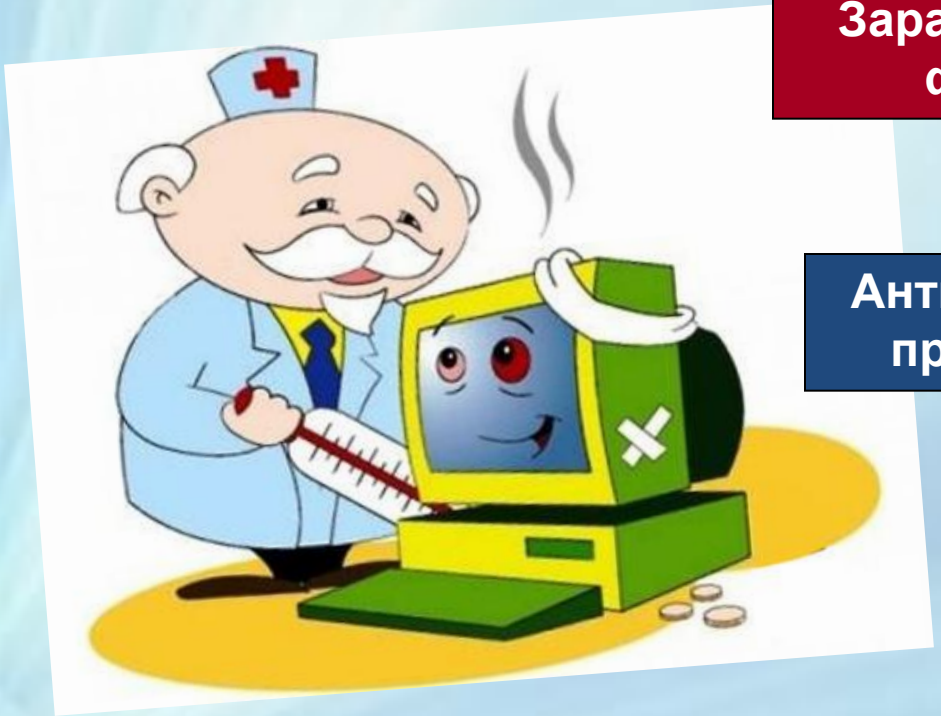
ПРОЦЕСС ЗАРАЖЕНИЯ ВИРУСОМ И ЛЕЧЕНИЯ ФАЙЛА

Компьютерный вирус → Незаражённая программа

Заражённый файл | Компьютерный вирус

Антивирусная программа

Вылеченный файл



Антивирусные сканеры -

это программы для сканирования системы на предмет выявления и удаления вредоносного ПО. Запуск происходит по требованию пользователя. Применяются в качестве дополнения и усиления действия основного антивируса, выявляя вредоносные программы пропущенные антивирусом.

Антивирусные мониторы -

это часть антивируса, предназначенная для непрерывного контроля ситуаций, при которых может произойти заражение вредоносной программой. Антивирусный монитор должен работать постоянно и в режиме реального времени, отслеживая потенциально опасные операции.

Рынок антивирусных программ очень разнообразен

Домашнее задание